# MATH 315; 3RD TEST

March 17, 2011

No aids such as calculators are allowed. Justify your answers. Answers without justification will be marked as zero.

**1.** (5 points) Let $p > 2$ be a prime number. What is the value of $1^3 + 2^3 + 3^3 + \cdots + (p-1)^3 \pmod{p}$?

**2.** (5 points) Determine whether or not the following congruence has a solution: $x^2 - 2x + 6 \equiv 0 \pmod{103}$. [Here 103 is a prime.]

**3.** (5 points) We know that 2 is a primitive root modulo 19. How many primitive roots modulo 19 are there? Represent them all in terms of the power of 2.

**4.** (5 points) Suppose that $a$ is a quadratic residue modulo a prime $p$, and suppose further that $p \equiv 5 \pmod 8$. Show that one of the values $x = a^{\frac{p+3}{8}}$ or $x = 2a\cdot(4a)^{\frac{p-5}{8}}$ is a solution to the congruence $x^2 \equiv a \pmod p$. [Hint: The second $x$ can be written as $x = 2^{\frac{p-1}{4}} a^{\frac{p+3}{8}}$, and $a^{\frac{p+3}{4}} = a^{\frac{p-1}{4}} \cdot a$]

**5.** (5 points) Starting from $259^2 + 1^2 = 34 \cdot 1973$, describe the Fermat's Descent Procedure to write the prime 1973 as a sum of two squares. You don't have to carry out the computation.

**6.** (5 points) For which primes $p > 3$ is $-3$ a quadratic residue modulo $p$, namely, when does $x^2 \equiv -3 \pmod p$ have a solution?